

all copied

1

one previously registered biometric sample for producing either a successful or failed identification of the user;

d. a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

2. The method of claim 1 wherein during the command execution step, the electronic rule module clearinghouse communicates with one or more third-party computers.

3. The method of claim 1 wherein said execution commands are comprised of any of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

4. The method of claim 1 wherein pattern data comprises any of the following; a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

5. The method of claim 1, wherein pattern data for a user is provided for the rule module by any of the following; the user, the electronic rule module clearinghouse, or an authorized third party.

6. The method of claim 1, wherein an execution command for a user is provided for the rule module by any of the following; the user, the electronic rule module clearinghouse, or an authorized third party.

7. The method of claim 1 further comprising a user re-registration check step, wherein the user's registration biometric sample is compared against previously registered biometric samples wherein if a match occurs, the computer system is alerted to the fact that the user has attempted to re-register with the electronic identicator.

8. The method of claim 1 wherein the biometric sample comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9. The method of claim 1 wherein during the identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

10. The method of claim 9 further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's biometric sample is determined to have been fraudulently duplicated.

11. The method of claim 1, wherein execution of an execution command authorizes the user to access stored electronic data.

12. The method of claim 11 wherein accessing stored electronic data results in activation of an Internet-connected device.

13. The method of claim 1 wherein executing an execution command processes electronic data to provide the user with a user requested electronic transmission.

14. The method of claim 13, wherein said processing comprises invoking any of the following: a user's digital certificate, a user's identity scrambler, a user's interactive electronic consumer loyalty or consumer rewards program, a user's interactive

electronic advertising, a user's interactive instant messaging program, a user's email authentication, and an automated electronic intelligent agent for electronic data search and retrieval that is customized to the user's requests.

15. The method of claim 1 wherein executing an execution command presents electronic data that is customized to the user's requested electronic transmission.

16. The method of claim 1 further comprising a user log-in repeat step, wherein during an electronic transmission the user is periodically required by the electronic identicator to present the user's bid biometric sample or at least one of the user's pattern data.

17. The method of claim 1 further comprising a communications step wherein any of the following is used: the Internet, an intranet, an extranet, a local area network, a wide area network.

18. The method of claim 1 further comprising a third-party registration step, wherein a third-party registers identification data with the electronic identicator, the identification data comprising any of the following; a biometric, a digital certificate, an Internet protocol address, or a biometric input apparatus hardware identification code.

19. The method of claim 18 further comprising a third-party identification step, wherein a third-party providing the user with electronic transmissions is identified by the electronic identicator by comparing the third-party's bid identification data with the third-party's registered identification data.

20. (First Amendment) A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:

- a. a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator; wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

*C25
cont'd
P 1*

- b. an electronic rule module clearinghouse, having at least one user-customizable rule module further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;
- c. an electronic identifier, for comparing the bid biometric sample with registered biometric samples of users;
- d. a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;

wherein no man-made memory tokens such as smartcards, or magnetic swipe cards are presented by the user to conduct the electronic transmission.

21. The device of claim 20 wherein the command execution module communicates with one or more third-party computers.

22. The device of claim 20 wherein pattern data comprises any of the following; a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

23. The device of claim 20, wherein pattern data for a user is provided for the rule module by any of the following; the user, the electronic rule module clearinghouse, or an authorized third party.

24. The device of claim 20, wherein an execution command for a user is provided for the rule module by any of the following; the user, the electronic rule module clearinghouse, or an authorized third party.

25 (First Amendment) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

- a. a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user, respectively;
- b. formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is associated with at least one execution command of the primary and subordinated user, the rule module customized to the primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user, and;
- c. a subordinated user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user;
- d. a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules;
- e. a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

26. The method of claim 3 wherein execution commands for accessing stored electronic data include permitting the user to access any of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts, and; restricted portions of corporate intranet databases.

27. The method of claim 26 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

28. The method of claim 26 wherein accessing membership benefits further comprises any of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site, and; validating a user's eligibility to enter a real-time internet chat room with other people on-line.

29. The method of claim 26 wherein accessing event admittance further comprises any of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres, and; validating a user's eligibility to board a vehicle of travel.

30. The method of claim 11 wherein accessing stored electronic data comprises accessing any of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content, and; server-based computer software programs and hardware drivers.

31. The method of claim 1 wherein at least one rule module further comprises any of the following: at least one pattern data associated with at least two execution commands, and; at least one execution command associated with at least two pattern data.

32. The method of claim 12 wherein activation of an internet-connected device further comprises activating any of the following devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine, and; a digital audio player.

33. The method of claim 14 wherein the automated intelligent agent for electronic data search and retrieval further comprises conducting periodic, user-customized on-line retrievals for any of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements and; faxes.

CH 31
34. (First Amendment) The method of claim 29 wherein the vehicle of travel further comprises any of the following: an airplane; a train; a boat; and, a bus.

35. The method of claim 14 wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

36. The method of claim 14 wherein invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

37. The method of claim 13 wherein the processing of electronic transmissions further comprises execution commands which filter the access and presentation of data when the user is subordinated user.

38. The method of claim 37 wherein the filter governs subordinated user access to any of the following: Internet web sites with adult content; internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user.

39. The device of claim 20 wherein execution commands for accessing stored electronic data include permitting the user to access any of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts, and; restricted portions of corporate intranet databases.

40. The device of claim 39 wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

41. The device of claim 39 wherein accessing membership benefits further comprises any of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site, and; validating a user's eligibility to enter a real-time internet chat room with other people on-line.

42. The device of claim 39 wherein accessing event admittance further comprises any of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres, and; validating a user's eligibility to board a vehicle of travel.

43. The device of claim 20 wherein execution commands further comprise accessing any of the following stored electronic data: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content, and; server-based computer software programs and hardware drivers.

44. The device of claim 20 wherein at least one rule module further comprises any of the following: at least one pattern data associated with at least two execution commands, and; at least one execution command associated with at least two pattern data.

45. The device of claim 20 wherein execution commands further comprise activation of any of the following internet-connected devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine, and; a digital audio player.

46. The device of claim 20 wherein execution commands further comprise an automated intelligent agent for electronic data search and retrieval which conducts periodic, user-customized on-line retrievals for any of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements and; faxes.

C5 *Sub 47* (First Amendment) The device of claim 42 wherein the vehicle of travel, further comprises any of the following: an airplane; a train; a boat; and, a bus.

48. The device of claim 46 wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

49. The device of claim 20 wherein execution commands further comprise invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

50. The device of claim 20 wherein execution commands further comprise the processing of electronic transmissions which filter the access and presentation of data when the user is subordinated user.

51. The device of claim 50 wherein the filter governs subordinated user access to any of the following: Internet web sites with adult content; internet sites with violent content;